APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/690,544	10/16/2000	Kenneth W. Aull	15-0216	2602

7590 11/10/2004		EXAMINER
Connie M. Thousand		PERUNGAVOOR, VENKATANARAY
TRW Inc.		
Law Dept.	ART UNIT	PAPER NUMBER
One Space Park, E2/6051	2132	
Redondo Beach, CA 90278		

DATE MAILED: 11/10/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	**Applicant(s)**
Office Action Summary	09/690,544	AULL ET AL.
	Examiner	**Art Unit**
	Venkatanarayanan Perungavoor	2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-66_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____ .

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____ .

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____ .

DETAILED ACTION

Claim Objections

1. The numbering of claims is not in accordance with 37 CFR 1.126 which requires the original numbering of the claims to be preserved throughout the prosecution. When claims are canceled, the remaining claims must not be renumbered. When new claims are presented, they must be numbered consecutively beginning with the number next following the highest numbered claims previously presented (whether entered or not).

2. Misnumbered claim 62-65 been renumbered 63-66. Applicant is requested to acknowledge the renumbering and to apply such in any response filed.

3. In Claim 62, the applicant mention claim 31 see Line 2, the examiner believes that the applicant intended claim 61, and interpreted the claim as such.

Claim Rejections – 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claim 1,7-9,32,38-40 rejected under 35 U.S.C. 102(e) as being anticipated by
U.S. Patent No. 6308277 B1 to Vaeth et al..

6. Regarding Claim 1, The "transmitting a role approval form, filled out and digitally
signed by the user using a personal digital signature, to at least one personal
role approval, signing digitally the role approval form by the personal role
approval using a personal digital signature, creating a role certificate upon receipt
of the role approval form signed by the user and the personal role approval,
notifying the user of the availability of the role certificate, and transmitting the role
certificate to the user" is met by Vaeth et al. see Column 4 Line 34- Line 54.

7. Regarding Claim 7, The "filling out an electronic form by a role member of the
plurality of role members of the group; signing digitally the electronic form by the
role member using the role certificate; signing digitally the electronic form by the
role member using a personal signature certificate; and transmitting the
electronic form to an entity" is met by Vaeth et al. see Column 4 Line 34- Line 54.

8. Regarding Claim 8, The "retrieving a policy associated with the role certificate by
the entity, and determining if the role certificate signature supplied is valid as a
signature for the electronic form" is met by Vaeth et al. see Column 3 Line 4-7 &
Column 3 Line 26-34.

9. Regarding Claim 9, The "transmitting a public key portion of the role certificate by the role member to the entity; encrypting information by the entity, transmitting the information to the role member, and decrypting the information by any member of the group having the digital certificate" is met by Vaeth et al. see Column 2 Line 65-Column 3 Line 6 & Column 3 Line 42-47.

10. Regarding Claim 32, The "transmitting a role approval form, filled out and digitally signed by the user using a personal digital signature, to at least one personal role approval, signing digitally the role approval form by the personal role approval using a personal digital signature, creating a role certificate upon receipt of the role approval form signed by the user and the personal role approval, notifying the user of the availability of the role certificate, and transmitting the role certificate to the user" is met by Vaeth et al. see Column 4 Line 34- Line 54.

11. Regarding Claim 38, The "filling out an electronic form by a role member of the plurality of role members of the group; signing digitally the electronic form by the role member using the role certificate; signing digitally the electronic form by the role member using a personal signature certificate; and transmitting the electronic form to an entity" is met by Vaeth et al. see Column 4 Line 34- Line 54.

12. Regarding Claim 39, The "retrieving a policy associated with the role certificate

by the entity, and determining if the role certificate signature supplied is valid as a

signature for the electronic form" is met by Vaeth et al. see Column 3 Line 4-7 &

Column 3 Line 26-34.

13. Regarding Claim 40, The "transmitting a public key portion of the role certificate

by the role member to the entity; encrypting information by the entity, transmitting

the information to the role member, and decrypting the information by any

member of the group having the digital certificate" is met by Vaeth et al. see

Column 2 Line 65-Column 3 Line 6 & Column 3 Line 42-47.

14. Claim 11-14,16-22,24,26-28,42-45,48-53,55,57-59,63-66 rejected under 35

U.S.C. 102(e) as being anticipated by U.S. Patent No. 6301658 B1 to Koehler.

15. Regarding Claim 11, The "displaying a list of roles to a user who is either a role

member or a role administrator, wherein the user is a member of a group

authorized to utilize the role certificate as a group stamp and for encryption of

information which may be decrypted by a plurality of group members, selecting a

role which is about to expire for renewal by the user; determining if the user is

authorized to renew the role based upon verification of the user's personal digital

signature, generating a new role certificate having a private and public key; and

transmitting the new role certificate to the user" is met by Koehler see Column 3

Line 12-19 & Column 3 Line 25-30.

16. Regarding Claim 12, The "the transmitting of the new role certificate to the user is

done over an encrypted secure communications line" is met by Koehler see

Column 5 Line 55-62.

17. Regarding Claim 13, The "transmitting of the new role certificate to the user the

new role certificate is transmitted to a certificate authority for approval and the

new role certificate is not transmitted to user without the approval" is met by

Koehler see Column 3 Line 45-48 & Column 3 Line 50-52.

18. Regarding Claim 14, The "public key portion of the role certificate is stored on a

server for access by individuals and entities outside of the group" is met by

Koehler see Column 2 Line 19-25.

19. Regarding Claim 16, Koehler discloses the use of "a public key, a private key, of

signature algorithm ID, validity period, extensions and at least one policy" see

Column 4 Line 66- Column 5 Line 5 & Column 6 Line 5-8.

20. Regarding Claim 17, The "transmitting a signature certificate to a registration web

server by a user; authenticating by accessing a directory that the user is still a

member of the organization, listing roles of which the user is a role member or a

role authority, and removing the role certificate associated with the role from a

directory database" is met by Koehler see Column 3 Line 12-19 & Column 3 Line

25-30.

21. Regarding Claim 18, The "role certificate is removed from the directory database

the role associated with the role certificate remains intact on the database" is met

by Koehler see Column 3 Line 27-30.

22. Regarding Claim 19, Koehler discloses "generating a new role certificate for the

role when the role certificate is removed from the directory database" see

Column 4 Line 2-6, "establishing a secure encrypted communications line with

the user; and transmitting the role certificate to the user" see Column 1 Line 62-

65.

23. Regarding Claim 20, Koehler discloses updating the members on the list, which

includes that which have been removed and new one that have been created see

Column 3 Line 61-Column 4 Line 6.

24. Regarding Claim 21, Koehler discloses the use of "a public key, a private key, of

signature algorithm ID, validity period, extensions and at least one policy" see

Column 4 Line 66- Column 5 Line 5 & Column 6 Line 5-8.

25. Regarding Claim 22, Koehler discloses transmitting of a digital signed certificate
and discloses that the certificate has been encrypted and that decryption
information is also known to receivers see Column 2 Line 5-15. And Koehler
discloses that an list that contains role members see Column 3 Line 11-13. And
further, Koehler discloses contacting authority for copy of the role certificate see
Column 4 Line 7-12 and transmitting the certificate Column 2 Line 23-25.

26. Regarding Claim 24, Koehler discloses the use of "a public key, a private key, of
signature algorithm ID, validity period, extensions and at least one policy" see
Column 4 Line 66- Column 5 Line 5 & Column 6 Line 5-8.

27. Regarding Claim 26, Koehler discloses transmitting an request to revoke an role
and its digital certificate that contains the signature see Column 6 Line 56-62.
Koehler discloses searching an list for all role certificates of an role see Column 8
Line 28-31.Koehler discloses having an list of role certificates that have been
revoked and selecting an role certificate to be removed and deleting it from the
list see Column 3 Line 25-30.

28. Regarding Claim 27,The deleting "from a directory when the role certificate and a
role are deleted from the database" is met by Koehler see Column 3 Line 12-14.

29. Regarding Claim 28, Koehler discloses the use of "a public key, a private key, of signature algorithm ID, validity period, extensions and at least one policy" see Column 4 Line 66- Column 5 Line 5 & Column 6 Line 5-8.

30. Regarding Claim 42, The "displaying a list of roles to a user who is either a role member or a role administrator, wherein the user is a member of a group authorized to utilize the role certificate as a group stamp and for encryption of information which may be decrypted by a plurality of group members, selecting a role which is about to expire for renewal by the user; determining if the user is authorized to renew the role based upon verification of the user's personal digital signature, generating a new role certificate having a private and public key; and transmitting the new role certificate to the user" is met by Koehler see Column 3 Line 12-19 & Column 3 Line 25-30.

31. Regarding Claim 43, The "the transmitting of the new role certificate to the user is done over an encrypted secure communications line" is met by Koehler see Column 5 Line 55-62.

32. Regarding Claim 44, The "transmitting of the new role certificate to the user the new role certificate is transmitted to a certificate authority for approval and the new role certificate is not transmitted to user without the approval" is met by Koehler see Column 3 Line 45-48 & Column 3 Line 50-52.

33. Regarding Claim 45, The "public key portion of the role certificate is stored on a

server for access by individuals and entities outside of the group" is met by

Koehler see Column 2 Line 19-25.

34. Regarding Claim 48, The "transmitting a signature certificate to a registration web

server by a user; authenticating by accessing a directory that the user is still a

member of the organization, listing roles of which the user is a role member or a

role authority, and removing the role certificate associated with the role from a

directory database" is met by Koehler see Column 3 Line 12-19 & Column 3 Line

25-30.

35. Regarding Claim 49, Koehler discloses the use of "a public key, a private key, of

signature algorithm ID, validity period, extensions and at least one policy" see

Column 4 Line 66- Column 5 Line 5 & Column 6 Line 5-8.

36. Regarding Claim 50, Koehler discloses "generating a new role certificate for the

role when the role certificate is removed from the directory database" see

Column 4 Line 2-6, "establishing a secure encrypted communications line with

the user; and transmitting the role certificate to the user" see Column 1 Line 62-

65.

37. Regarding Claim 51, Koehler discloses updating the members on the list, which includes that which have been removed and new one that have been created see Column 3 Line 61-Column 4 Line 6.

38. Regarding Claim 52, Koehler discloses the use of "a public key, a private key, of signature algorithm ID, validity period, extensions and at least one policy" see Column 4 Line 66- Column 5 Line 5 & Column 6 Line 5-8.

39. Regarding Claim 53, Koehler discloses transmitting of a digital signed certificate and discloses that the certificate has been encrypted and that decryption information is also known to receivers see Column 2 Line 5-15. And Koehler discloses that an list that contains role members see Column 3 Line 11-13. And further, Koehler discloses contacting authority for copy of the role certificate see Column 4 Line 7-12 and transmitting the certificate Column 2 Line 23-25.

40. Regarding Claim 55, Koehler discloses the use of "a public key, a private key, of signature algorithm ID, validity period, extensions and at least one policy" see Column 4 Line 66- Column 5 Line 5 & Column 6 Line 5-8.

41. Regarding Claim 57, Koehler discloses transmitting an request to revoke an role and its digital certificate that contains the signature see Column 6 Line 56-62.

Koehler discloses searching an list for all role certificates of an role see Column 8

Line 28-31.Koehler discloses having an list of role certificates that have been

revoked and selecting an role certificate to be removed and deleting it from the

list see Column 3 Line 25-30.

42. Regarding Claim 58, The deleting "from a directory when the role certificate and

a role are deleted from the database" is met by Koehler see Column 3 Line 12-

14.

43. Regarding Claim 59, Koehler discloses the use of "a public key, a private key, of

signature algorithm ID, validity period, extensions and at least one policy" see

Column 4 Line 66- Column 5 Line 5 & Column 6 Line 5-8.

44. Regarding Claim 63, The "a public key, a private key, a signature algorithm ID, a

validity period extensions include encryption and signature, and a policy" is met

by Koehler see Column 4 Line 66-Column 5 Line 5 & Column 6 Line 5-8.

45. Regarding Claim 64, Koehler discloses the decrypting of encrypted information

see Column 1 Line 63-66. And Koehler discloses the digital signature given by an

authority on behalf of an organization or group see Column 5 Line 14-20.

46. Regarding Claim 65, Koehler discloses that an certificate is given to each role member and that it role member receives certificates that are particular to his/her group only with certain defined roles and role member can't access the roles see Column 2 Line 55-67.

47. Regarding Claim 66, Koehler discloses verifying the certificate and including of information by the authority whereby the information is an digital signature see Column 5 Line 17-20.

48. Claim 29,30,60,61 rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6487658 B1 to Micali.

49. Regarding Claim 29, Micali discloses identifying an role certificate to be recovered and searching to find whether the role is still valid; transmitting a request for approval by recovery agent and receiving an approval; transmitting the role certificate to user see Column 25 Line 20-34. The transmiting of role certificate to an agent is disclosed by Micali see Column 24 Line 67-Column 25 Line 6.

50. Regarding Claim 30, Micali discloses two agents that must approve before a role certificate is provided see Column 25 Line 37-49.

51. Regarding Claim 60, Micali discloses identifying an role certificate to be

recovered and searching to find whether the role is still valid; transmitting a

request for approval by recovery agent and receiving an approval; transmitting

the role certificate to user see Column 25 Line 20-34. The transmiting of role

certificate to an agent is disclosed by Micali see Column 24 Line 67-Column 25

Line 6.

52. Regarding Claim 61, Micali discloses two agents that must approve before a role

certificate is provided see Column 25 Line 37-49.

Claim Rejections – 35 USC § 103

53. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in

section 102 of this title, if the differences between the subject matter sought to be patented and the prior art

are such that the subject matter as a whole would have been obvious at the time the invention was made to

a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be

negatived by the manner in which the invention was made.

54. Claim 2-6,10,33-37,41 rejected under 35 U.S.C. 103(a) as being unpatentable

over U.S. Patent No. 6308277 B1 to Vaeth et al. in view of U.S. Patent No.

6275859 B1 to Wesley et al.

55. Regarding Claim 2, Vaeth et al. does not disclose role certificate comprises a public key, a private key, of signature algorithm ID, validity period, extensions and at least one policy". However Wesley et al. discloses the use of public key, a private key, validity period, extensions and policies and identifier of the roles see Column 4 Line 18-Line 27. It would be obvious to one having ordinary skill in the art at the time of the invention to include to role certificate a public key, a private key, of signature algorithm ID, validity period, extensions and at least one policy in order to provide identities and authorization to participate in session see Column 3 Line 6-Line 9.

56. Regarding Claim 3, The "policy indicates all permitted uses and limitations on the role certificate" is met by Vaeth et al. see Column 4 Line 4-Line 11.

57. Regarding Claim 4, The "identifying all members of a group as role members that will access and use of the role certificate, storing the names and identifications of all role members, and transmitting copies of the role certificate to all role members" is met by Vaeth et al. see Column 4 Line 38-44 & Column 4 Line 58-61.

58. Regarding Claim 5, The "transmitting the public key portion of the role certificate to a plurality of entities outside the group; and decrypting messages from the

plurality of entities outside the group encrypted using the public key portion of the

role certificate" is met by Vaeth et al. see Column 3 Line 42-47.

59. Regarding Claim 6, The "signing electronic forms by a group member utilizing the

role certificate; and transmitting electronic forms to entities outside the group" is

met by Vaeth et al. see Column 4 Line 44-49.

60. Regarding Claim 10, Vaeth et al. does not disclose "role certificate comprises a

public key, a private key, of signature algorithm ID, validity period, extensions

and at least one policy, wherein the extensions indicate that the role certificate

may be used for both encryption and as a digital signature". However Wesley et

al. discloses role certificate comprises a public key, a private key, validity period,

and other information that identify the role and also discloses that it may be used

for both encrypted and as a digital signature see Column 4 Line 17-27 & Column

2 Line 10-14. It would be obvious to one having ordinary skill in the art at the time

of the invention to include to role certificate a public key, a private key, validity

period, and other information that identify the role and that it may be used for

both encrypted and as a digital signature in order for reliable data that provides

security and avoiding availability and performance problems see Column 2 Line

54-58.

61. Regarding Claim 33, Vaeth et al. does not disclose "role certificate comprises a public key, a private key, of signature algorithm ID, validity period, extensions and at least one policy, wherein the extensions indicate that the role certificate may be used for both encryption and as a digital signature". However Wesley et al. discloses role certificate comprises a public key, a private key, validity period, and other information that identify the role and also discloses that it may be used for both encrypted and as a digital signature see Column 4 Line 17-27 & Column 2 Line 10-14. It would be obvious to one having ordinary skill in the art at the time of the invention to include to role certificate a public key, a private key, validity period, and other information that identify the role and that it may be used for both encrypted and as a digital signature in order for reliable data that provides security and avoiding availability and performance problems see Column 2 Line 54-58.

62. Regarding Claim 34, The "policy indicates all permitted uses and limitations on the role certificate" is met by Vaeth et al. see Column 4 Line 4-Line 11.

63. Regarding Claim 35, The "identifying all members of a group as role members that will access and use of the role certificate, storing the names and identifications of all role members, and transmitting copies of the role certificate to all role members" is met by Vaeth et al. see Column 4 Line 38-44 & Column 4 Line 58-61.

64. Regarding Claim 36, The "transmitting the public key portion of the role certificate

   to a plurality of entities outside the group; and decrypting messages from the

   plurality of entities outside the group encrypted using the public key portion of the

   role certificate" is met by Vaeth et al. see Column 3 Line 42-47.

65. Regarding Claim 37, The "signing electronic forms by a group member utilizing

   the role certificate; and transmitting electronic forms to entities outside the group"

   is met by Vaeth et al. see Column 4 Line 44-49.

66. Regarding Claim 41, Vaeth et al. does not disclose "role certificate comprises a

   public key, a private key, of signature algorithm ID, validity period, extensions

   and at least one policy, wherein the extensions indicate that the role certificate

   may be used for both encryption and as a digital signature". However Wesley et

   al. discloses role certificate comprises a public key, a private key, validity period,

   and other information that identify the role and also discloses that it may be used

   for both encrypted and as a digital signature see Column 4 Line 17-27 & Column

   2 Line 10-14. It would be obvious to one having ordinary skill in the art at the time

   of the invention to include to role certificate a public key, a private key, validity

   period, and other information that identify the role and that it may be used for

   both encrypted and as a digital signature in order for reliable data that provides

security and avoiding availability and performance problems see Column 2 Line

54-58.

67. Claim 15,46,47 rejected under 35 U.S.C. 103(a) as being unpatentable over U.S.

Patent No. 6301658 B1 to Koehler in view of U.S. Patent No. 6308277 B1 to

Vaeth et al.

68. Regarding Claim 15, Koehler does not disclose "the private key portion of

the role certificate is stored in a key recovery authority". However Vaeth et al.

discloses the storage of private keys see Column 8 Line 13-23. It would be

obvious to one having ordinary skill in the art at the time of the invention to

include an storage of private keys for recovery in order for them to be accesed by

other networks or special hardwares and softwares see Column 8 Line 23-28.

69. Regarding Claim 46, Koehler does not disclose "the private key portion of

the role certificate is stored in a key recovery authority". However Vaeth et al.

discloses the storage of private keys see Column 8 Line 13-23. It would be

obvious to one having ordinary skill in the art at the time of the invention to

include an storage of private keys for recovery in order for them to be accesed by

other networks or special hardwares and softwares see Column 8 Line 23-28.

70. Regarding Claim 47, Koehler discloses the use of "a public key, a private key, of signature algorithm ID, validity period, extensions and at least one policy" see Column 4 Line 66- Column 5 Line 5 & Column 6 Line 5-8.

71. Claim 23,25,54,56 rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6301658 B1 to Koehler in view of U.S. Patent No. 6275859 B1 to Wesley et al.

72. Regarding Claim 23, Koehler does not disclose authenticating that the role member is either a member of the role or a role authority for the role prior to contacting the key recovery authority. However, Wesley et al. discloses verifying of role prior to the contacting recovery authority see Column 4 Line 3-6 & Column 4 Line 15-17. It would be obvious to one having ordinary skill in the art at the time of the invention to include verifying of role prior to the contacting recovery authority in order operation to be performed before session not during active session and thus increasing latency see Column 4 Line 12-14.

73. Regarding Claim 25, The "all members of the role are informed of the role certificate" is met by Koehler see Column 4 Line 39-44.

74. Regarding Claim 54, Koehler does not disclose authenticating that the role member is either a member of the role or a role authority for the role prior to

contacting the key recovery authority. However, Wesley et al. discloses verifying

of role prior to the contacting recovery authority see Column 4 Line 3-6 & Column

4 Line 15-17. It would be obvious to one having ordinary skill in the art at the time

of the invention to include verifying of role prior to the contacting recovery

authority in order operation to be performed before session not during active

session and thus increasing latency see Column 4 Line 12-14.

75. Regarding Claim 56, The "all members of the role are informed of the role

certificate" met by Koehler see Column 4 Line 39-44.

76. Claim 31,62 rejected under 35 U.S.C. 103(a) as being unpatentable over U.S.

Patent No. 6487658 B1 to Micali in view U.S. Patent No. 6275859 B1 to Wesley

et al.

77. Regarding Claim 31, Micali does not disclose agents being authenticated prior to

the role certificate being sent to the recovery agent. However, Wesley et al.

discloses verifying of role prior to the contacting recovery agent see Column 4

Line 3-6 & Column 4 Line 15-17. It would be obvious to one having ordinary skill

in the art at the time of the invention to include verifying of role prior to the

contacting recovery authority in order operation to be performed before session

not during active session and thus increasing latency see Column 4 Line 12-14.

78. Regarding Claim 62, Micali does not disclose agents being authenticated prior to

the role certificate being sent to the recovery agent. However, Wesley et al.

discloses verifying of role prior to the contacting recovery agent see Column 4

Line 3-6 & Column 4 Line 15-17. It would be obvious to one having ordinary skill

in the art at the time of the invention to include verifying of role prior to the

contacting recovery authority in order operation to be performed before session

not during active session and thus increasing latency see Column 4 Line 12-14.

Conclusion

79. The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

The following patents are cited to further show the state of art in general

    U.S. Patent No. 6438691 B1 to Mao

    U.S. Patent No. 6675296 B1 to Boeyen et al.

    U.S. Patent No. 6813714 B1 to Hardjono et al.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Venkatanarayanan Perungavoor whose

telephone number is 571-272-7213. The examiner can normally be reached on

8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone

number for the organization where this application or proceeding is assigned is

703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR

only. For more information about the PAIR system, see http://pair-

direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-

free).

VP

Venkatanarayanan Perungavoor

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100